
Certificate Issuing and Management Components

Protection Profile

NIST PKI Project Team

TABLE OF CONTENTS

1	INTRODUCTION.....	1
1.1	IDENTIFICATION.....	1
1.2	OVERVIEW.....	1
1.2.1	<i>CIMC Keys.....</i>	<i>1</i>
1.2.2	<i>Data Input.....</i>	<i>2</i>
1.2.3	<i>Trusted Public Key Entry, Deletion, and Storage.....</i>	<i>3</i>
1.2.4	<i>CIMC Security Levels.....</i>	<i>3</i>
1.2.5	<i>Requirements Overview.....</i>	<i>4</i>
2	TOE DESCRIPTION.....	5
3	TOE SECURITY ENVIRONMENT	5
3.1	SECURE USAGE ASSUMPTIONS	5
3.2	THREATS.....	6
3.3	ORGANIZATIONAL SECURITY POLICIES	8
4	SECURITY OBJECTIVES.....	8
4.1	SECURITY OBJECTIVES FOR THE TOE.....	8
4.2	NON-IT SECURITY OBJECTIVES.....	12
4.3	NON-TOE IT SECURITY OBJECTIVES	12
5	SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT	12
6	TOE SECURITY FUNCTIONAL REQUIREMENTS.....	13
6.1	SECURITY AUDIT (MANDATORY)	14
6.2	ROLES (MANDATORY).....	20
6.3	BACKUP AND RECOVERY (MANDATORY).....	23
6.4	ACCESS CONTROL (MANDATORY).....	25
6.5	IDENTIFICATION AND AUTHENTICATION (I&A) (MANDATORY).....	27
6.6	REMOTE DATA ENTRY AND EXPORT	29
6.6.1	<i>Certificate Status Export (Mandatory).....</i>	<i>31</i>
6.7	KEY MANAGEMENT.....	32
6.7.1	<i>Key Generation (Mandatory).....</i>	<i>32</i>
6.7.2	<i>Private Key Load and Storage (Mandatory).....</i>	<i>32</i>
6.7.3	<i>Public Key Storage (Mandatory).....</i>	<i>33</i>
6.7.4	<i>Secret Key Storage.....</i>	<i>33</i>
6.7.5	<i>Private and Secret Key Destruction (Mandatory).....</i>	<i>34</i>
6.7.6	<i>Private and Secret Key Export.....</i>	<i>34</i>
6.8	SELF-TESTS (MANDATORY)	35
6.9	CERTIFICATE PROFILE MANAGEMENT (MANDATORY)	37
6.10	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	38
6.11	ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) PROFILE MANAGEMENT	39
6.12	CERTIFICATE REGISTRATION (MANDATORY)	39
6.13	CERTIFICATE REVOCATION.....	41
6.13.1	<i>Certificate Revocation List Validation.....</i>	<i>41</i>
6.13.2	<i>OCSP Basic Response Validation.....</i>	<i>41</i>
6.14	CRYPTOGRAPHIC MODULES.....	42
6.15	OPERATING SYSTEM	42
6.16	STRENGTH OF FUNCTION	43
6.16.1	<i>Authentication Mechanisms.....</i>	<i>43</i>
6.16.2	<i>Cryptographic Modules</i>	<i>43</i>

7	TOE SECURITY ASSURANCE REQUIREMENTS.....	45
7.1.1	<i>Security Level 1 Security Assurance</i>	<i>45</i>
7.1.2	<i>Security Level 2 Security Assurance</i>	<i>46</i>
7.1.3	<i>Security Level 3 Security Assurance</i>	<i>47</i>
7.1.4	<i>Security Level 4 Security Assurance</i>	<i>47</i>
8	RATIONALE.....	48
8.1	IT SECURITY OBJECTIVES RATIONALE	48
8.2	NON-IT SECURITY OBJECTIVES RATIONALE	50
8.3	FUNCTIONAL SECURITY REQUIREMENTS RATIONALE.....	50
8.4	SECURITY POLICY RATIONALE	53
9	CIMC ACCESS CONTROL POLICY.....	55
10	(PRELIMINARY) GLOSSARY OF TERMS.....	56
11	ACRONYMS	59

1 INTRODUCTION

1.1 Identification

Title: Certificate Issuing and Management Components (CIMCs) Protection Profile

Registration: TBD

Keywords: Public Key Infrastructure, PKI, Certificate Issuing and Management Component, CIMC

1.2 Overview

A Public Key Infrastructure (PKI) is an architecture that is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings and provide other services critical to managing public keys. A PKI consists of many components. A Certificate Issuing and Management System (CIMS) includes the components of the PKI that are responsible for the issuance, revocation, and overall management of certificates and certificate status information. A CIMS always includes a Certification Authority (CA) and may include Registration Authorities (RAs) and other subcomponents.

A Certificate Issuing and Management Component (CIMC) consists of the hardware, software, and firmware that are responsible for performing the functions of a CIMS. A CIMC does not include environmental controls (e.g., controlled access facility, temperature), policies and procedures, personnel controls (e.g., background checks and security clearances), and other administrative controls.

This Protection Profile (PP) specifies the functional and assurance security requirements for a CIMC. The intent of this requirements document is to ensure specification of the complete set of requirements for a CIMC and not the specification of a subset of requirements implemented in a specific CIMC subcomponent. It includes all the technical features of a CIMC, regardless of which CIMC subcomponent performs the function. The document does not differentiate between functions that are typically performed by a CA and functions that are typically performed by a RA.

Identifying all the subcomponents of a CIMC as a single entity assists in ensuring that the subcomponents compliant with the security requirements in this document will operate in a secure manner. This approach also ensures compatibility because a single vendor (or integrator) typically develops (or bundles) all the subcomponents together as a single solution. Typically, this is consistent with the way products are currently designed and built. A single product solution may make purchasing decisions easier because the user (or procurer) will not need to select subcomponents that meet a subset of the requirements. Finally, a single solution approach promotes security because the CIMC must:

- Implement all the mandatory security requirements, regardless of how they are allocated to subcomponents, and
- Ensure that functions implemented in one subcomponent do not compromise the security functions implemented in other subcomponents.

1.2.1 CIMC Keys

It is essential that private and secret keys in CIMCs be managed securely. For the purposes of this document, keys are separated into three categories based on the individual or device that is authorized to use the key:

1. *CIMS personnel keys*: Private and secret keys used within a CIMC designated for use by individual identities. CIMS personnel keys may be used for authentication, to sign information contained within or output by a CIMC, or to encrypt information files.
2. *Component keys*: Keys, other than CIMS personnel keys, which are used by the CIMC. CIMCs shall use Component keys to sign certificates and certificate status information. Component public/private key pairs may also be used in key agreements, for signing audit logs and system

backups and for ensuring the integrity of transmitted or stored data. Component secret keys may be used to encrypt CIMC stored or transmitted data and compute authentication codes.

3. *Certificate subject private keys*: Private keys corresponding to the public keys contained in certificates issued by the CIMC where:
 - the private key is held by the CIMC solely to enable key recovery; or
 - the CIMC generates a public/private key pair and the private key is only held by the CIMC until the certificate subject has received it.

1.2.1.1 Cryptographic Functions Involving Private or Secret Keys

Private and secret keys within a CIMC are separated into different usage categories as described below. Listed in brackets next to each usage category are the associated key user categories defined in the CIMC Keys section.

1. *Certificate and Status Signing Keys*: Private keys used to sign certificates, CRLs, or other statements about the status of certificates. [Component keys]
2. *Integrity or Approval Authentication Keys*: Private or secret keys used to protect the integrity of transactions between CIMCs or CIMC subcomponents. Private or secret keys used to authenticate transactions between CIMCs that cause or approve the issuance or revocation of certificates. [CIMS personnel keys, Component keys]
3. *General Authentication Keys*: Private or secret keys used to authenticate users, messages, or sessions that do not include the authorization or approval of certificate issuance or revocation, but may include requests to issue or revoke certificates. [CIMS personnel keys, Component keys]
4. *Long Term Private Key Protection Keys*: Secret or private keys that are used to protect private keying material that is used for multiple sessions or messages. [CIMS personnel keys, Component keys]
5. *Long Term Confidentiality Keys*: Secret keys that are used to protect the confidentiality of security-relevant information such as PINS or passwords. This information does not include private keying material. [CIMS personnel keys, Component keys]
6. *Short Term Private Key Protection Keys*: Private keys used to protect keying material for a single session or message. [CIMS personnel keys, Component keys]
7. *Short Term Confidentiality Keys*: Secret keys used to protect a single session or message that does not contain keying material. [CIMS personnel keys, Component keys]

1.2.2 Data Input

A CIMC may receive information in many different ways. Data input is organized in the following three categories depending on the source of the data (local or remote) and whether the user is authenticated by the CIMC.

1. *Unauthenticated Data Entry*: The message/data may either be entered locally or received over a network. The originator of the message/data cannot be verified i.e., the user is unauthenticated.
2. *Local Data Entry*: A user, operating locally, enters or accepts data so that the CIMC can associate the data with the user and list the user in the audit log with the accepted data. The data entry could take the form of a user vouching for information that has already been entered into the computer by clicking on an “accept” button or by otherwise indicating acceptance of the information.
3. *Remote Data Entry*: The data could be received over a network in such a way that it can be bound to the identity of the sender of the data (or to the identity of some other remote user). For example, the data could be sent in a signed email.

1.2.3 Trusted Public Key Entry, Deletion, and Storage

In addition to issuing public key certificates, CIMCs may use public keys for their own purposes. Specifically, a CIMC may use the public key of another entity to encrypt messages that it intends to send to that entity, authenticate messages that it receives from that entity, or perform a key agreement to establish a session key for communicating with that entity.

A public key may be trusted by a CIMC because it is contained in a certificate that was issued by a CA that the CIMC trusts. At the next level, trust in the public key used to verify the signature on that certificate must be established. Trust in this public key may be established by another certificate. This trust validation *path* will continue until the final (or root) public key is reached. In order to bootstrap the process at the root public key, a CIMC must establish trust in this public key through some means other than certificate path processing. While the signatures on public key certificates authenticate and protect most public keys, a digital signature does not protect these public key “trust anchors”. Also, these public keys must be protected from modification.

Every CIMC that uses public keys for authentication, encryption, integrity, or access control will maintain a list of trusted public keys. This list may include several keys (e.g., one for each authorized user) or may include only one key, which can be used to verify trust in all other public keys through path validation.

1.2.4 CIMC Security Levels

CIMCs will be operated in a wide variety of environments, from a closed secure facility to an open access facility in a hostile environment. Also, the sensitivity of the information protected by the certificates issued by CIMCs will vary significantly. Users will be required to evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity of the information. To address the varying levels of risk, this document specifies security requirements at four increasing, qualitative levels of security: Security Level 1, Security Level 2, Security Level 3, and Security Level 4.

1.2.4.1 Security Level 1

Security Level 1 provides the lowest level of security. CIMCs designed to meet the security requirements at Security Level 1 may be appropriate for use in environments in which the threat of malicious activity is considered to be low. CIMCs at Security Level 1 do not provide protection against unauthorized disclosure by malicious authorized or unauthorized users. At this Level, the CIMC provides functions appropriate to a PKI. All cryptographic algorithms must be FIPS-approved and the cryptographic module validated against FIPS 140-1, *Security Requirements for Cryptographic Modules*. Security Level 1 requires, at a minimum, two distinct roles. One role will be responsible for account administration, key generation, audit configuration and a second role responsible for issuing and revoking certificates. These responsibilities must be divided between two (or more) separate, mutually exclusive, roles. Security Level 1 should be achievable using currently available products. Security Level 1 differs from higher levels in several aspects; for example, all cryptographic functions to be performed by cryptographic modules must be validated only to FIPS 140-1 Security Level 1.

At Security Level 1, the CIMC is evaluated at the Common Criteria (CC) Evaluation Assurance Level (EAL) 1 with the addition of Functional Testing. The objective of this assurance level is to provide evidence that the CIMC functions as specified in the associated documentation.

1.2.4.2 Security Level 2

CIMCs designed to meet Security Level 2 may be appropriate where the risks and consequences of data disclosure are not significant. CIMCs at Security Level 2 should defend against most attacks initiated through a network. It is assumed at this security level that the users of the PKI are not malicious. Security Level 2 requires, at a minimum, two distinct roles. One role will be responsible for account administration, key generation, audit configuration and a second role responsible for issuing and revoking certificates. These responsibilities must be divided between two (or more) separate, mutually exclusive, roles. Security

Level 2 increases the number of events that must be audited and requires increased cryptographic protection of audit logs and system backups. In addition, FIPS 140-1 level 2 cryptographic modules are required for the protection of some private keying material.

At Security Level 2, the CIMC is evaluated against the assurance requirements specified in *CSPP – Guidance for COTS Security Protection Profiles*. The assurance requirements of CSPP stress assurance through vendor actions that are currently within best commercial practices.

1.2.4.3 Security Level 3

CIMCs designed to meet Security Level 3 may be appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. Level 3 requires additional integrity controls to ensure data is not modified. A CIMC at Security Level 3 includes protections to protect against someone with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

This security level provides some protection against malicious authorized users by requiring, at a minimum, three distinct roles. One role will be responsible for account administration, key generation, and audit configuration; a second role will be responsible for issuing and revoking certificates; and a third role responsible for maintaining the audit logs. Security Level 3 requires two-party control of private key export and additional auditing of import and export of secret and private keys and requests for information. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140-1 Security Level 3. Finally, there is increased public key protection and digital signatures are required on all messages.

At Security Level 3, the applicable CC assurance requirements are extracted from EAL3 (methodically tested and checked) and EAL4 (methodically designed, tested and reviewed). The majority of the requirements are from EAL3. An EAL3 evaluation provides an analysis supported by “gray box” testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities.

1.2.4.4 Security Level 4

CIMCs designed to meet Security Level 4 may be appropriate where the threats to and consequences of data disclosure and loss of data integrity are significant. The environment and the users may be hostile. Security Level 4 is intended to protect against malicious authorized and unauthorized users. This is partly accomplished by requiring, at a minimum, four distinct roles. One role will be responsible for account administration and key generation; a second role responsible for maintaining the audit logs; a third role responsible for issuing and revoking certificates; and a fourth role responsible for performing backups. A Security Level 4 CIMC requires significant assurance that the security features are functioning properly. Security Level 4 increases the integrity of audit logs by requiring signed third-party timestamping. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140-1 level 4. Security Level 4 products are currently not available, but should be achievable in the next few years.

At Security Level 4, the applicable CC assurance requirements are extracted from EAL4 (methodically designed, tested and reviewed) and EAL5 (semiformally designed and tested). The majority of the requirements are from EAL4. EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices, supported by moderate application of specialized security engineering techniques.

1.2.5 Requirements Overview

All CIMCs must implement the mandatory requirements and functions. Requirements and functions that are not specifically marked as mandatory are optional. However, if a CIMC implements an optional function, the CIMC must implement the security requirements specified in the document for that function.

Security requirements are also separated according to the Security Level for which they are applicable. Unless otherwise specified, the security requirements in each subsection apply to all four Security Levels.

2 TOE DESCRIPTION

The CIMC Protection Profile (CIMCPP) defines a set of security requirements to be levied on Targets of Evaluation (TOEs). These TOEs include information systems that include general purpose operating systems. A CIMC TOE may be a stand-alone system or consist of components in a network or distributed environment. A CIMC TOE permits one or more processors and associated peripherals and storage devices to be used by multiple users to perform a variety of PKI functions requiring controlled, shared access to the information stored on the system.

All individual users are assigned a unique identifier. This identifier supports individual accountability.

3 TOE SECURITY ENVIRONMENT

3.1 *Secure Usage Assumptions*

Authorized Users

A.Auditors Review Audit Logs

Audit logs are required for security-relevant events and must be reviewed by the Auditors.

A.Authenticated Roles

Administrators, Operators, Officers and Auditors are authenticated and held accountable for their actions.

A.Competent Administrators, Operators, Officers and Auditors

Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

A.Cooperative Users

Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner. (Levels 1–3).

A.No Abusive Administrators, Operators, Officers and Auditors

Administrators, Operators, Officers and Auditors are trusted not to abuse their authority. (Levels 1-2)

A.Remote Secure Administration

Administrators, Operators, Officers and Auditors have remote access and are able to view and modify security-relevant data. (Addressed at Levels 3-4, only)

A.Remote Users

Users are permitted to access the TOE by remote means. This access is trusted not to compromise the security of the TOE.

System Failures

A.Authentication Data Management

Authentication data management is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)

A.Corruption of System Data

Users cannot accidentally overwrite any system programs, logs, or data.

A.Disposal of Authentication Data

Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).

External Attacks**A.Communications Protection**

The system is adequately physically protected against loss of communications i.e., availability of communications.

A.Hardware Integrity

The system shall include integrity mechanisms to provide for the detection of hardware modifications.

A.Natural Disaster Protection

The system is adequately protected against natural disasters such as fires and floods (e.g., sprinkler systems, alarms, etc.)

A.Physical Protection

The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification. (Levels 1-2)

3.2 Threats**Authorized Users****T.Administrators, Operators, Officers and Auditors commit errors**

An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application. (Addressed at Levels 3-4, only)

T.Administrative errors of omission

Administrators, Operators, Officers or Auditors fail to perform some function essential to security.

T.Hostile Administrator, Operator, Officer or Auditor actions

An Administrator, Operator, Officer or Auditor maliciously modifies the system's configuration to allow security violations to occur. (Addressed at Levels 3-4, only)

T.Hostile user acts cause confidentiality breaches

A user collects sensitive or proprietary information and removes it from the system, either by putting it on a disk or by transmitting it outside the organization. (Addressed at Levels 3-4, only)

T.User abuses authorization to collect data

User abuses granted authorizations to improperly collect sensitive or security-critical data. (Addressed at Levels 3-4, only)

T.User abuses authorization to send data

User abuses granted authorizations to improperly send sensitive or security-critical data.

T.User error makes data inaccessible

User accidentally deletes user data rendering user data inaccessible.

T.User's misuse causes denial of service

Users unauthorized use of resources causes undue burden on an affected resource.

System Failures

T.Critical system component fails

Failure of one or more system components results in the loss of system critical functionality.

T.Flawed code

A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

T.Malicious code exploitation

An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. (Addressed at Level 4, only)

T.Message content modification

A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.

T.TOE developed with inadequate TSF self protection

System or applications developer delivers code that includes security flaws that prevent the TSF from adequately protecting itself. The security flaws may be either deliberate or accidental.

Cryptography**T.Disclosure of private and secret keys**

A private or secret key is improperly disclosed.

T.Modification of private/secret keys

A secret/private key is modified.

T.Sender denies sending information

The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction. (Addressed at Levels 3-4, only)

T.Weak cryptographic algorithms

Cryptographic algorithms that have not been tested against a known standard may be weak and, consequently, may be broken.

External Attacks**T.Hacker masquerading as a legitimate user or as system process**

A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process. (Addressed at Level 4, only)

T.Hacker physical access

A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

T.Hacker undetected system access

A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability. (Addressed at Level 4, only)

T.Outsider eavesdrops on user data communications

An outsider obtains user data by eavesdropping on communications lines. (Addressed at Level 4, only)

T.Social engineering

A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation. (Addressed at Levels 3-4, only)

3.3 Organizational Security Policies

P.Authorized use of information

Information shall be used only for its authorized purpose(s).

P.Cryptography

FIPS-approved cryptographic algorithms shall be implemented.

P.Individual accountability

Individuals shall be held accountable for their actions.

P.Information access control

Only authorized individuals and processes shall access information.

P.Information availability

Information shall be available to satisfy mission requirements.

P.Information content integrity.

Information shall retain its content integrity.

P.Installation and usage guidance

Guidance shall be provided for the secure installation and use of the system.

P.Notification of threats and vulnerabilities

Appropriate authorities shall be notified of any threats or vulnerabilities impacting systems that process their data. (Levels 3-4)

P.System lifecycle phases integrate security

Information systems security shall be an integral part of all system lifecycle phases.

4 SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

Authorized Users

O.Administrators, Operators, Officers and Auditors guidance documentation

Deter Administrator, Operator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.

O.Auditor role

Deter modification or destruction of data (and other potential vulnerabilities) through the creation of an Auditor role.

O.Audit records with identity

Record in audit records: date and time of action, location of the action, and the entity responsible for the action.

O.Auditing for user accountability

Provide information about user activities for user accountability.

O.Certificates

The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.

O.Detect modifications of backup hardware, firmware, and software

Provide integrity protection to detect modifications to backup hardware, firmware, and software.

O.Protected user authentication data

Execute protection measures (e.g., cryptography) to ensure that either user authentication data cannot be accessed, or when it is accessed, it cannot be used to gain access to the system.

O.Guarantee the availability of audit storage space

Maintain audit data and guarantee space for that data.

O.Individual accountability

Provide individual accountability for audited events.

O.Limitation of administrative access control

Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions.

O.Maintain user attributes

Maintain a set of security attributes (which may include role membership, access privileges, etc.) associated with individual users. This is in addition to user identity.

O.Notify authorities of security issues

Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data. (Assurance provided at Levels 3 and 4)

O.Operator/Administrator access

Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.

O.Respond to possible loss of stored audit records

Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.

O.Restrict actions before authentication

Restrict the actions a user may perform before the TOE verifies the identity of the user.

O.Security roles

Maintain security-relevant roles and the association of users with those roles.

O.Security-relevant configuration management

Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.

O.Tamper detection

Detect tampering with the system and notify appropriate personnel.

O.User authorization management

Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.

System Failures

O.Apply patches to fix the code

Apply patches to fix the code when vulnerabilities in code allow, for example, unauthorized and undetected access.

O.Authorization

The TSF must ensure that only authorized users gain access to the TOE and its resources.

O.Code signing and verification

Check verification of signed downloaded code prior to execution.

O.Configuration Management

Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.

O.Enforcement

The TSF must be designed and implemented in a manner that ensures that the organizational policies are enforced in the target environment.

O.Examine source code for developer flaws

Examine for accidental or deliberate flaws in code made by the developer. The deliberate flaws include building trap doors.

O.Integrity protection of user data and software

Provide appropriate integrity protection for user data and software.

O.Isolate untrusted executables

Run untrusted executable code in a separate domain where potential errors or embedded malicious code will not significantly impact other system functions of other valid users of the system. (Addressed at Level 4, only)

O.Lifecycle security

Provide tools and techniques used during the development phase to ensure security is designed into the CIMC. Detect and resolve flaws during the operational phase.

O.Local detection of received security-relevant data modified in transit

Identification by the system (TOE) of modification of security relevant (TSF) data occurring in transit.

O.Manage behavior of security functions

Provide management functions to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code

Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.

O.Periodically check integrity

Provide periodic integrity checks on both system and user data.

O.Preservation of secure state for failures in critical components

Preserve the secure state of the system in the event of a secure component failure.

O.Procedures for preventing malicious code

Incorporate malicious code prevention procedures and mechanisms.

O.Protect stored audit records

Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

O.Protect user data during internal transfer

Ensure the integrity of user data transferred internally within the system.

O.Require inspection for downloads

Require inspection of downloads/transfers.

O.Sufficient backup storage and effective restoration

Provide sufficient backup storage and effective restoration to ensure that the system can be recreated.

O.Time stamps

Provide time stamps to ensure that the sequencing of events can be verified.

O.Trusted recovery of security functionality

After a discontinuity of operations recover to a secure state.

O.Validation of security function

Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

Cryptography

O.Cryptographic algorithms

The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification.

O.Key generation

Implement approved key generation techniques.

O.Non-repudiation

Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message. (Assurance provided at Levels 3 and 4.)

O.Robust encryption

Use approved encryption products/modules. (Approved is defined as FIPS 140-1 validated.)

External Attacks

O.Audit system access to deter misuse

Audit system access to discover system misuse.

O.Control unknown source communication traffic

Control (e.g., reroute or discard) communication traffic from an unknown source to prevent potential damage.

O.Data Import/Export

Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

O.General user documentation

Provide documentation for the general user and for the administrative roles.

O.Guarantee the availability of audit storage space

Maintain audit data and guarantee space for that data.

O.Identify and authenticate each user

Uniquely identify and authenticate each user of the system.

O.Manage security-relevant data

Manage the initialization of, values for, limits on, and allowable operations on security-relevant data to ensure the secure operation of the CIMC.

O.React to detected attacks

Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent. (Addressed at Levels 3-4, only)

O.Trusted Path

Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities. (Addressed at Levels 3-4, only)

4.2 Non-IT Security Objectives

O.Administrative Training

Administrators, Operators, Officers and Auditors are trained to define, implement, and maintain effective security practices.

O.CPS

All Administrators, Operators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practice statement (CPS) that describes the TOE.

O.Credentials

Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which maintains IT security.

O.Installation

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

O.Physical Protection

Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.

4.3 Non-TOE IT Security Objectives

TBD

5 Security Requirements for the IT Environment

Users cannot bypass the security mechanisms of the TOE. The underlying system will provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with.

Software sent from outside sources must be handled to protect against the inclusion of unauthorized software, for example, viruses and trojan horses.

Provide through frequent audits, restoration of security-relevant changes to the system between backup and restore, and restoration of the security-relevant system state (e.g., access control list) without destruction of other system data.

Provide through frequent backups, restoration of system changes between backup and restore. Every CIMC will have a certification practice statement (CPS) and a certificate policy (CP) that documents the operation of the CIMC.

6 TOE Security Functional Requirements

This section specifies the security requirements that are applicable to CIMC functionality, such as key management, certificate registration, and CIMC configuration and management functions. The CIMC requirements are specified by level. If a requirement is listed without levels, the requirement applies to all four levels.

This section includes the *basic security requirements*. These are the requirements that are applicable to all functions implemented in the CIMC. These requirements are roles, audit, backup and recovery, and identification and authentication.

Table 1 lists all the CC functional security requirements that are included in this PP. They are listed in alphabetical order in Table 1 for ease of reference. Also included is the applicable CIMC PP section.

Table 1. CIMC Functional Security Requirements

CC Functional Requirement	CIMC PP Section
FAU_GEN.1 Audit data generation	6.1 Security Audit
FAU_GEN.2 User identity association	6.1 Security Audit
FAU_SAR.1 Audit Review	6.1 Security Audit
FAU_SAR.3 Selectable audit review	6.1 Security Audit
FAU_SEL.1 Selective audit	6.1 Security Audit
FAU_STG.1 Protected audit trail storage	6.1 Security Audit
FAU_STG.4 Prevention of audit data loss	6.1 Security Audit
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	6.6 Remote Data Entry and Export
FCO_NRO_CIMC.4 Advanced verification of origin	6.6 Remote Data Entry and Export
FCS_CKM.1 Cryptographic key generation	6.7 Key Management
FCS_CKM.4 Cryptographic key destruction	6.7 Key Management
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	6.7 Key Management
FCS_COP.1 Cryptographic operation	6.13 Cryptographic Modules
FDP_ACC.1 Security attribute based access control	6.4 Access Control
FDP_ACF_CIMC.2 User private key confidentiality protection	6.7 Key Management
FDP_ACF_CIMC.3 User secret key confidentiality protection	6.7 Key Management
FDP_CIMC_BKP.1 CIMC backup and recovery	6.3 Backup and Recovery
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	6.3 Backup and Recovery
FDP_CIMC_BKP.3 Advanced CIMC backup and recovery	6.3 Backup and Recovery
FDP_CIMC_CER.1 Certificate Generation	6.11 Certificate Registration
FDP_CIMC_CRL.1 Certificate Revocation	6.12 Certification Revocation
FDP_CIMC_CSE.1 Certificate status export	6.6 Remote Data Entry and Export
FDP_ETC_CIMC.4 User private and secret key export	6.7 Key Management
FDP_ETC_CIMC.5 Extended user private and secret key export	6.7 Key Management
FDP_ITT.1 Basic internal transfer protection	6.6 Remote Data Entry and Export
FDP_SDI_CIMC.3 Stored public key	6.7 Key Management

CC Functional Requirement	CIMC PP Section
integrity monitoring and action	
FDP_UCT.1 Basic data exchange confidentiality	6.6 Remote Data Entry and Export
FIA_AFL.1 Authentication failure handling	6.5 Identification and Authentication
FIA_ATD.1 User attribute definition	6.5 Identification and Authentication
FIA_UAU.1 Timing of authentication	6.5 Identification and Authentication
FIA_UID.1 Timing of identification	6.5 Identification and Authentication
FIA_USB.1 User-subject binding	6.5 Identification and Authentication
FMT_MOF.1 Management of security functions behavior	6.2 Roles
FMT_MOF_CIMC.2 Certificate profile management	6.9 Certificate Profile Management
FMT_MOF_CIMC.3 Extended certificate profile management	6.9 Certificate Profile Management
FMT_MOF_CIMC.4 Certificate revocation list profile management	6.10 Certificate Revocation List Profile Management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	6.10 Certificate Revocation List Profile Management
FMT_MSA.1 Management of security attributes	6.2 Roles
FMT_MSA.2 Secure security attributes	6.2 Roles
FMT_MSA.3 Static attribute initialization	6.2 Roles
FMT_MTD.1 Management of TSF data	6.2 Roles
FMT_MTD_CIMC.4 TSF private key confidentiality protection	6.7 Key Management
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	6.7 Key Management
FMT_MTD_CIMC.6 TSF private and secret key export	6.7 Key Management
FMT_MTD_CIMC.7 Extended TSF private and secret key export	6.7 Key Management
FMT_SMR.2 Restrictions on security roles	6.2 Roles
FPT_AMT.1 Abstract machine testing	6.8 Self Tests
FPT_CIMC_TSP.2 Audit log signing event	6.1 Security Audit
FPT_CIMC_TSP.2 Audit log time stamp event	6.1 Security Audit
FPT_ITC.1 Inter-TSF confidentiality during transmission	6.6 Remote Data Entry and Export
FPT_ITT.1 Basic internal TSF data transfer protection	6.6 Remote Data Entry and Export
FPT_STM.1 Reliable time stamps	6.1 Security Audit
FPT_TST_CIMC.2 Software/firmware integrity test	6.8 Self Tests
FPT_TST_CIMC.3 Software/firmware load test	6.8 Self Tests
FPT_TRP.1 Trusted path	6.5 Identification and Authentication

6.1 Security Audit (Mandatory)

Audit includes a chronological recording of events that occur in a system. The objective is to track what occurs to enable the reconstruction and examination of a sequence of events and/or changes in an event. This is useful in ensuring that the system is operated securely and in providing evidence when a suspected

or actual security compromise has occurred. Audit also provides for reconstructing a specific state of a system. The objective in a PKI system is to enable an appropriate authority to determine whether a signature should have been accepted as valid.

The audit will be used to reconstruct important events that were performed by the CIMC, such as issuance of a CA certificate, and the user or event (e.g., a signed certificate request) that caused them. The audit will be used to arbitrate future disputes by establishing the validity of a signature at a particular time.

The audit log records the security-relevant events that were performed by the CIMC and the users or events (e.g., a signed certificate request) that caused them. This subsection specifies the security requirements for maintaining and protecting the integrity of the audit logs. If the audit requirements are addressed by the underlying operating system, they do not need to be separately addressed by the CIMC.

The CIMC may maintain either a single audit log or multiple audit logs. If multiple audit logs are used then the CIMC may either maintain a different audit log at each of the physically separated parts of the CIMC (e.g., the CA may maintain an audit log in addition to each of the RAs) or may divide audit entries among the audit logs based on the type of event being audited (e.g., audit entries that are to be maintained for a very long time may be placed in a separate audit log to be used as an archive). If multiple audit logs are maintained, then each event to be audited (as specified in FAU_GEN.1) must be included in at least one of the audit logs. All other audit requirements apply to each audit log.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the **basic???** level of audit; and
- c) The events listed in Table 2 below.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, the information specified in the Additional Details column in Table 2 below.

FAU_GEN.1.3 The audit shall not include plaintext private or secret keys or other critical security parameters.

Dependencies: FPT_STM.1 Reliable time stamps

Table 2. Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
6.1: Security Audit	FAU_GEN.1 Audit data generation	Any changes to the audit parameters, e.g., audit frequency, type of event audited	
		Any attempt to delete the audit log	
	FPT_CIMC_TSP.1 Audit log time stamp event	Obtaining a third party time stamp	The digitally signed third party timestamp shall be included in the audit log.
6.5: Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a role	
	FIA_AFL.1	The value of <i>maximum</i>	

Section/Function	Component	Event	Additional Details
	Authentication failure handling	<i>authentication attempts</i> is changed (Levels 2, 3, 4)	
		<i>Maximum authentication attempts</i> unsuccessful authentication attempts occur during user login (Levels 2, 3, 4)	
	FIA_AFL.1 Authentication failure handling	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts (Levels 2, 3, 4)	
		An Administrator changes the type of authenticator, e.g., from password to biometrics (Levels 2, 3, 4)	
Local Data Entry		All security-relevant data that is entered in the system	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an “accept” button). This shall be included with the accepted data.
Remote Data Entry		All security-relevant messages that are received by the system	
Data Export and Output		All successful and unsuccessful requests for confidential and security-relevant information (Levels 2, 3, 4)	
6.7.1: Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the CIMC generates a key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
6.7.2: Private Key Load and Storage		The loading of Component private keys	
		All access to certificate subject private keys retained within the CIMC for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
6.7.4: Secret Key Storage		The manual entry of secret keys used for authentication (Levels 3 and 4)	
6.7.6: Private and Secret Key Export	FDP_ETC_CIMC.4 User private and secret key export; FMT_MTD_CIMC.6 TSF private and	The export of private and secret keys (keys used for a single session or message are excluded)	

Section/Function	Component	Event	Additional Details
	secret key export		
6.11: Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
6.12: Certificate Revocation	FDP_CIMC_CRL.1 Certificate Revocation	All certificate revocation requests+	
Certificate Status Change Approval		The approval or rejection of a certificate status change request	
CIMC Configuration		Any security-relevant changes to the configuration of the CIMC	
Account Administration		Roles and users are added or deleted	
		The access control privileges of a user account or a role are modified	
6.9: Certificate Profile Management	FMT_MOF_CIMC.2 Certificate profile management; FMT_MOF_CIMC.3 Extended certificate profile management	All changes to the certificate profile	The changes made to the profile
Revocation Profile Management		All changes to the revocation profile	The changes made to the profile
6.10: Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide *Auditors* with the capability to read [ST assignment: *list of audit information*] from the audit records.

Application Note: The ST author should specify the type of information the specified user is permitted to obtain from the audit records. Examples are “all”, “subject identity”, “all information belonging to audit records referencing this user”.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform searches of audit data as specified in Table 3 below.

Dependencies: FAU_SAR.1 Audit review

Table 3. Audit Search Criteria

Section/Function	Component	Search Criteria
6.1: Security Audit	FAU_GEN.1 Audit data generation	The type of the event and the identity of the user responsible for causing the event
Certificate Request Remote and Local Data Entry		Identity of the subject of the certificate being requested
Certificate Revocation Request Remote and Local Data Entry		Identity of the subject of the certificate to be revoked

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

- a) [selection: *object identity, user identity, subject identity, host identity, event type*]
- b) [assignment: *list of additional attributes that audit selectivity is based upon*].

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

Dependencies: FAU_GEN.1 Audit data generation

NOTE: One method of meeting the requirements of FAU_STG.1 is to write audit data directly to non-modifiable media.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the Auditor, if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

SECURITY LEVELS 2 and 3

In addition to the above security requirements, FPT_CIMC_TSP.1 shall apply to CIMCs at Security Levels 2 and 3.

FPT_CIMC_TSP.1 Audit log signing event

Hierarchical to: No other components.

FPT_CIMC_TSP.1.1 The TOE shall periodically create an audit log signing event in which it computes a digital signature, keyed hash, or authentication code over the entries in the audit log.

FPT_CIMC_TSP.1.2 The digital signature, keyed hash, or authentication code shall be computed over, at least, every entry that has been added to the audit log since the previous audit log signing event and the digital signature, keyed hash, or authentication code from the previous audit log signed event.

FPT_CIMC_TSP.1.3 The specified frequency at which the audit log signing event occurs shall be configurable.

FPT_CIMC_TSP.1.4 The digital signature, keyed hash, or authentication code from the audit log signing event shall be included in the audit log.

Dependencies: FAU_GEN.1

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.protect stored audit records, by providing additional protection for stored audit records at Security Levels 2 and 3.

SECURITY LEVEL 4

In addition to the above security requirements, FPT_CIMC_TSP.2 shall apply to CIMCs at Security Level 4.

FPT_CIMC_TSP.2 Audit log time stamp event

Hierarchical to: No other components.

FPT_CIMC_TSP.2.1 The TSF shall obtain a digitally signed third party timestamp at a specified frequency.

FPT_CIMC_TSP.2.2 The digital signature of the third party timestamp shall be computed over, at least, every entry that has been added to the audit log since the previous third party timestamp was generated and the digital signature from the previous third party timestamp.

FPT_CIMC_TSP.2.3 The digital signature shall not be computed by the TOE.

FPT_CIMC_TSP.2.4 The specified frequency at which the TOE obtains a third party timestamp shall be configurable.

FPT_CIMC_TSP.2.5 The digitally signed third party timestamp shall be included in the audit log.

Dependencies: FAU_GEN.1

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.protect stored audit records, by providing additional protection for stored audit records at Security Level 4.

6.2 Roles (Mandatory)

The ability to perform many of the functions specified in this PP will be allocated to distinct roles to maintain the security of a CIMC. This subsection defines a set of roles that will be used throughout this document when allocating responsibilities.

A CIMC is not required to implement all of the roles listed, but is only required to implement roles to meet the role separation requirements. A single identity may be assigned multiple roles except where prohibited by the CIMC requirements. Multiple individuals may be assigned to a specific role, as required by the CIMC implementation.

The role definitions are listed below:

1. *Administrator* – role authorized to install, configure, and maintain the CIMC; establish and maintain user accounts; configure profiles and audit parameters; and generate Component keys.
2. *Operator* – role authorized to perform system backup and recovery.
3. *Officer* – role authorized to request or approve certificates or certificate revocations.
4. *Auditor* – role authorized to view and maintain audit logs.

It is important that one individual cannot perform all the functions specified for a CIMC. One mechanism to deter abuse of power is the separation of CA duties.

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1

FMT_SMR.2 has different requirements for security levels 1 and 2, security level 3, and security level 4.

SECURITY LEVELS 1 AND 2

FMT_SMR.2.1 The TSF shall maintain the roles Administrator and Officer.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that no identity is authorized to assume both an Administrator and an Officer role.

SECURITY LEVEL 3

FMT_SMR.2.1 The TSF shall maintain the roles Administrator, Auditor, and Officer.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that:

- a) no identity is authorized to assume both an Administrator and an Officer role;
- b) no identity is authorized to assume both an Auditor and an Officer role; and
- c) no identity is authorized to assume both an Administrator and an Auditor role.

SECURITY LEVEL 4

FMT_SMR.2.1 The TSF shall maintain the roles Administrator, Auditor, Officer, and Operator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that no identity is authorized to assume more than one of the role specified above.

Dependencies: FIA_UID.1 Timing of identification

NOTE: If a CIMC does not implement one of the roles specified above (e.g., Auditor or Operator), then the capabilities assigned to that role by this Protection Profile must be assigned to some other role or roles.

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in Table 4 to the authorized roles.

Dependencies: FMT_SMR.1 Security roles

Table 4: Authorized roles for management of security functions behavior

Section/Function	Component	Event
6.1: Security Audit		<p>The capability to configure the audit parameters shall be restricted to Administrators.</p> <p>The capability to change the frequency of the audit log signing event shall be restricted to Administrators. (Levels 2-4).</p> <p>The capability to change the frequency of the timestamping event or the source of the timestamp shall be restricted to Administrators. (Level 4)</p>
6.3: Backup and Recovery		<p>The capability to configure the backup parameters shall be restricted to Administrators.</p> <p>The capability to initiate the backup or recovery function shall be restricted to Operators.</p>
6.6: Identification and Authentication		<p>The capability to specify or change <i>maximum authentication attempts</i> shall be restricted to Administrators.</p> <p>The capability to change authentication mechanisms shall be restricted to Administrators.</p>
6.12: Certificate Registration		<p>The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers.</p> <p>If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Officers.</p>
Data Export and Output		<p>The export of CIMC private keys shall require the authorization of at least two Administrators. (Security Levels 3 and 4)</p>
Certificate Status Change Approval		<p>Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate.</p> <p>Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.</p>
CIMC		<p>The capability to configure any CIMC functionality</p>

Section/Function	Component	Event
Configuration		shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the CIMC functionality has been assigned to a different role elsewhere in this document.)
Account Administration		The capability to create user accounts and roles shall be restricted to Administrators. The capability to assign privileges to those accounts and roles shall be restricted to Administrators.
6.10: Certificate Profile Management	FMT_MOF_CIMC.2 Certificate profile management; FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administrators.
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
6.11: Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the CIMC access control policy to restrict the ability to modify the security attributes [ST assignment: *list of security attributes*] to Administrators.

Application Note: The ST must state components of the security attributes that may be modified and any restrictions that may exist for Administrators. The ST must state the components of the access rights that the Administrator is allowed to modify.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security Roles

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the CIMC access control policy to provide [ST selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the SFP.

Application Note: The TSF shall provide default values for relevant object security attributes, which can be overridden by an initial value. It may be possible for a new object to have different security attributes at creation, if a mechanism exists to specify the permissions at time of creation. The ST author should select whether the default property of the access control attribute will be restrictive, permissive, or another property. In case of another property, the ST author should refine this to a specific property.

FMT_MSA.3.2 The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to view (read) or delete the audit logs to Auditors.

Dependencies: FMT_SMR.1 Security roles

6.3 Backup and Recovery (Mandatory)

Backup and recovery includes reconstructing a system in the event of a system failure or other serious error.

In order to be able to recover from failures and other unanticipated undesired events, CIMCs must be able to back up the system. The backup will be used to restore the CIMC to an operational status at a previous point in time. The frequency of performing backups (e.g., hourly, daily, or weekly) is based on the criticality of the application or system. The backup and recovery requirements may be addressed by the underlying CIMC operating system.

FDP_CIMC_BKP.1 CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.1.1 The TSF shall include a backup function.

FDP_CIMC_BKP.1.2 The Operator shall be capable of invoking the backup function on demand.

FDP_CIMC_BKP.1.3 The data stored in the system backup shall be sufficient to recreate the state of the system at the time the backup was created using only:

- i. a copy of the same version of the CIMC as was used to create the backup data;
- ii. a stored copy of the backup data;
- iii. the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and
- iv. the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.

FDP_CIMC_BKP.1.4 The TSF shall include a recovery function that is able to restore the state of the system from a backup.¹

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Security roles.

SECURITY LEVELS 2 and 3

In addition to the above requirements, FDP_CIMC_BKP.2 shall apply to CIMCs at Security Levels 2 and 3.

FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.2.1 The backup data shall be protected against modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_CIMC_BKP.2.2 Critical security parameters and other confidential information shall be stored in encrypted form only.

Dependencies: FDP_CIMC_BKP.1 CIMC backup and recovery

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.security roles.

SECURITY LEVEL 4

In addition to the requirements at Security Levels 2 and 3, FDP_CIMC_BKP.3 shall apply to CIMCs at Security Level 4.

FDP_CIMC_BKP.3 Advanced CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.3.1 The TSF shall maintain sufficient information to recreate the state of the system at the time of the last completed CIMC transaction using only:

- i. a copy of the same version of the CIMC as was used to create the backup data;
- ii. a stored copy of the backup data from the most recently created system backup;
- iii. any data maintained by the CIMC in non-volatile storage (e.g., magnetic disk or tape or other storage device whose contents are preserved when power is off);
- iv. the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and
- v. the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.

¹ NOTE: The recovery function, in restoring the state of the system, is only required to create an “equivalent” system state in which information about all relevant CIMC transactions has been maintained.

FDP_CIMC_BKP.3.2 The recovery function of the TSF shall be capable of recreating the state of the system at the time of the last completed transaction. The recovery function shall reflect only completed transactions.

Dependencies: FDP_CIMC_BKP.1 CIMC backup and recovery
FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.security roles.

6.4 Access Control (Mandatory)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the CIMC access control policy on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Application Note: The terms object and subject refer to generic elements in the TOE. For a policy to be implementable, these entities must be clearly identified. For most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST. For a PP, the objects and operations might be expressed as types such as: named objects, data repositories, observe accesses, etc. The ST author should specify the list of subjects, objects, and operations among subjects and objects covered by the SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the CIMC access control policy to objects based on the identity of the subject and the set of roles that the subject is authorized to assume.

FDP_ACF.1.2 The TSF shall enforce the rules specified in Table 5 to determine if an operation among controlled subjects and controlled objects is allowed.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [ST assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

Application Note: The rules that govern the CIMC access control policy may vary between TOEs; those rules need to be specified in the ST. The ST must list the attributes that are used for access decisions. These attributes may include permission bits, access control lists, and object ownership. The ST author should specify the rules, based on security attributes, that explicitly **authorize** access of subjects to objects. These rules are in addition to those specified in FDP_ACF.1.1. They are included in FDP_ACF.1.3 as they are intended to contain exceptions to the rules in FDP_ACF.1.1.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [ST assignment: *rules, based on security attributes that explicitly deny access of subjects to objects*].

Application Note: The rules that govern the CIMC access control policy may vary between TOEs; those rules need to be specified in the ST. The ST must list the attributes that are used for access decisions. These attributes may include permission bits, access control lists, and object ownership. The ST author should specify the rules, based on security attributes, that explicitly **deny** access of subjects to objects. These rules are in addition to those specified in FDP_ACF.1.1. They are included in FDP_ACF.1.4 as they are intended to contain exceptions to the rules in FDP_ACF.1.1.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

Table 5: Access controls

Section/Function	Component	Event
Certificate Request Remote and Local Data Entry		The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry		The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked.
Data Export and Output		The export or output of confidential and security-relevant data shall only be at the request of authorized users.
6.8.1: Key Generation	FCS_CKM.1 Cryptographic Key Generation	The capability to generate Component keys (used to protect data in more than a single session or message) shall be restricted to Administrators.
6.8.2: Private Key Load and Storage		<p>The capability to load Component private keys into cryptographic modules shall be restricted to Administrators.</p> <p>The capability to decrypt certificate subject private keys within a CIMC shall be restricted to Officers.</p> <p>The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures.</p> <p>At least two Officers shall be required to decrypt certificate subject private keys. (Security Levels 3 and 4)</p>
Trusted Public Key Entry, Deletion, and Storage		The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators.
6.8.4: Secret Key Storage		The capability to load CIMC secret keys into cryptographic modules shall be restricted to Administrators.
6.8.5: Private and Secret Key Destruction		The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators, Auditors, Officers, and Operators.
6.8.6: Private and Secret Key Export		<p>The capability to export a component private key shall be restricted to Administrators.</p> <p>The capability to export certificate subject private keys shall be restricted to Officers.</p> <p>The export of a certificate subject private key shall require the authorization of at least two Officers. (Levels 3 and 4) (See note below)</p>

Section/Function	Component	Event
Certificate Status Change Approval ²		<p>Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold.</p> <p>Only Officers shall be capable of removing a certificate from on hold status.</p> <p>Only Officers shall be capable of approving the placing of a certificate on hold.</p> <p>Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate.</p> <p>Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.</p>

NOTE: It has been brought to our attention that this may pose a problem for CIMCs that generate key pairs for their certificate subjects. The original intention was to require two-party control for key recovery operations. However, as written, this requirement also applies to the initial export of a centrally generated private key for the purposes of delivering the private key to the certificate subject. While we believe that two-party control for key recovery is important at Security Levels 3 and 4, this requirement may be overly burdensome for high-volume CIMCs that generate key management key pairs for their certificate subjects. We would appreciate suggestions in the area.

6.5 Identification and Authentication (I&A) (Mandatory)

Identification and authentication includes recognizing an entity (e.g., user, device, or system) and verifying the identity of that entity. The I&A requirements may be addressed by the underlying CIMC operating system.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: the set of roles that the user is authorized to assume, [ST assignment: *other security attributes*].

Application Note: The specified attributes are those that are required by the TSF to enforce the CIMC access control policy, the generation of audit records, and proper identification and authentication of users. The user identity must be uniquely associated with a single individual user. Group membership may be expressed in a number of ways: a list per user specifying to which groups the user belongs, a list per group which includes which users are members, or implicit association between certain user identities and certain groups. The ST author should specify the security attributes that are associated with an individual user. An example of such a list is { 'clearance', 'group identifier', 'rights' }.

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

² Every request to change certificate status, for example, revoke a certificate, place a certificate on hold, or remove a certificate from hold must be accepted or rejected. If a request is accepted, any information about the request that may be exported from the CIMC must be approved. Approval may be manual or automated.

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [ST assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [ST assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application Note: FIA_UAU.1 and FIA_UID.1 allow the ST author to specify TSF-mediated actions that may be performed on behalf of a user before that user is identified and/or authenticated. However, the TOE shall not perform any security-relevant functions or export/output any confidential information on behalf of a user before that user has been identified or authenticated. Examples of TSF-mediated actions that may be performed on behalf of a user before that user is identified and/or authenticated include:

- a) Responding to a request for public information (e.g., responding to an Online Certificate Status Protocol (OCSP) request).
- b) Accepting data from a user that will not be processed until an (identified and authenticated) authorized user has accepted the data (e.g., a unauthenticated user may submit a certificate request message so long as the certificate is not generated until after an Officer has approved the request).

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User attribute definition

SECURITY LEVEL 2

In addition to the I&A requirements specified above, FIA_AFL.1 shall also apply for Security Level 2.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable *maximum authentication attempts* unsuccessful authentication attempts have occurred since the last successful authentication for the indicated user identity.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [ST assignment: *list of actions*].

Application Note: The ST must specify the actions to be taken in case the threshold is met or surpassed. These actions could be disabling of an account for five minutes or

disabling of the account until unlocked by the administrator and simultaneously informing the administrator. (In order to prevent a denial-of-service attack, accounts that belong to Administrators should not be disabled.) The actions should specify the measures and, if applicable, the duration of the measure (or the conditions under which the measure will be ended).

Dependencies: FIA_UAU.1 Timing of authentication

SECURITY LEVELS 3 AND 4

In addition to the I&A requirements specified for Security Levels 1 and 2, FTP_TRP.1 shall apply for Security Levels 3 and 4.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

- FTP_TRP.1.1** The TSF shall provide a communication path between itself and [ST selection: *local, local and remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
- FTP_TRP.1.2** The TSF shall permit [ST selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.
- FTP_TRP.1.3** The TSF shall require the use of the trusted path for initial user authentication, [ST assignment: *other services for which trusted path is required*].

Application Note: The ST should identify other services for which a trusted path is required, if any. A trusted path may be required for any security-relevant interaction.

Dependencies: No dependencies

6.6 Remote Data Entry and Export

This section covers cases in which data is to be associated with a user who is not acting locally. In most cases, this will involve data that has been received in a message that has been signed or that contains an authentication code or keyed hash allowing the source of the message to be determined (in which case the data may be associated with the source of the message). Data received over a secure communication channel (e.g., SSL) could be treated similarly.

The security requirements of remote data entry apply whenever data has been received from a remote source that is considered reliable (i.e., the source of the information can be determined). These requirements also apply to communications between physically distributed parts of a single CIMC over an untrusted network (e.g., receipt of a signed certificate request message by a CA from an RA would be considered a message receipt even if the RA and CA were being validated as a single CIMC).

This section also specifies security requirements associated with the export of data from CIMCs. The data may be distributed to a device that is outside the boundary of a CIMC (either locally or remotely). The remote device or computer may not be directly connected to the CIMC. Data export also applies when data is sent between physically distributed subcomponents of a CIMC (e.g., data sent between a CA and RA) and the data is transmitted over an untrusted network. Data export does not apply to data sent to a printer or monitor that is inside the CIMC boundary.

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

Hierarchical to: FCO_NRO.2

- FCO_NRO_CIMC.3.1** The TSF shall enforce the generation of evidence of origin for certificate status information and all other security-relevant information at all times.

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity and [ST assignment: *other attributes*] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

Application Note: The ST shall specify the list of other attributes that shall be linked to the information, for example, time of origin and location of origin.

FCO_NRO_CIMC.3.3 The TSF shall verify the evidence of origin of information for all security-relevant information.

Dependencies: FIA_UID.1 Timing of identification

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.Non-repudiation.

NOTE: Based on FCO_NRO_CIMC.3, the TSF shall reject any information whose origin can not be verified unless:

- a) Acceptance of the information will not cause the TSF to perform any security relevant functions; and
- b) Acceptance of the data will not cause the TSF to output or export any confidential information.

The TSF may, for example, accept information whose origin can not be verified under in the following cases:

- a) The received information is a request for public information (e.g., an Online Certificate Status Protocol (OCSP) request).
- b) The received information will not be processed until an authorized user has accepted its contents (e.g., a certificate request). In this case, the received information may be processed as if it had originated from the authorized user who approved it.

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the CIMC access control policy to prevent the modification of security-relevant user data and the disclosure of confidential user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the CIMC access control policy to be able to transmit objects in a manner protected from unauthorized disclosure.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 The TSF shall protect confidential TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect security-relevant TSF data from modification when it is transmitted between separate parts of the TOE.

FPT_ITT.1.1 The TSF shall protect confidential TSF data from disclosure when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

SECURITY LEVELS 3 AND 4

In addition to the above Remote Data Entry and Export requirements, FCO_NRO_CIMC.4 shall apply to CIMCs at Security Levels 3 and 4.

FCO_NRO_CIMC.4 Advanced verification of origin

Hierarchical to: No other components.

FCO_NRO_CIMC.4.1 The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using an authentication code, keyed hash, or digital signature algorithm.

FCO_NRO_CIMC.4.2 The TSF shall, for all other security-relevant information, only accept the information if it was signed using a digital signature algorithm.

Dependencies: FCO_NRO_CIMC.3

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.Non-repudiation.

6.6.1 Certificate Status Export (Mandatory)

All CIMCs must be capable of exporting certificate status information. Any message sent by a CIMC containing certificate status information must meet the requirements for Certificate Status Export in addition to the requirements for Data Export specified in section 6.6.

The following requirements apply to Certificate Status Export.

FDP_CIMC_CSE.1 Certificate status export

Hierarchical to: No other components

FDP_CIMC_CSE.1.1 If a message indicates the status of a certificate and the certificate is within its period of validity, then the message shall indicate the certificate's current status (e.g., valid, revoked, on hold).

FDP_CIMC_CSE.1.2 The status of a certificate shall be valid unless a change in status has been approved.

FDP_CIMC_CSE.1.3 If certificate status is output on a certificate revocation list (CRL), then the CRL shall be compliant with the X.509 standard.

FDP_CIMC_CSE.1.4 If certificate status is output as an Online Certificate Status Protocol (OCSP) response, then the OCSP response shall be compliant with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2560.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7 Key Management

Cryptographic keys are used by CIMCs for many different reasons: to ensure the integrity of messages sent over untrusted networks, to authenticate users, to protect the confidentiality of private information, and to protect the confidentiality of stored information such as audit logs. As such, the unauthorized modification, disclosure, or substitution of any of these cryptographic keys could result in a loss of security.

Keys have a life cycle that begins with their generation. After generation, keys are stored, activated, deactivated, and destroyed. In many cases, keys are backed up and audited. Typically, public keys are distributed. In some cases, private and secret keys are distributed.

6.7.1 Key Generation (Mandatory)

This subsection specifies the requirements for the generation of cryptographic keys by CIMCs.

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in a cryptographic module that is in a FIPS-approved mode of operation. Certificate subject private keys shall be generated by a cryptographic module that meets the overall Security Level specified for Long Term Private Key Protection Keys (see Table 6). All other cryptographic keys shall be generated by a cryptographic module that meets the Security Level required for the use of the key (see Table 6).

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

6.7.2 Private Key Load and Storage (Mandatory)

Private keys may be used by a CIMC for many different purposes and stored for long periods. CIMCs may store Component keys, CIMS personnel keys, and, for key recovery purposes, certificate subject private keys.

FDP_ACF_CIMC.2 User private key confidentiality protection

Hierarchical to: No other components

FDP_ACF_CIMC.2.1 CIMS personnel private keys shall be stored in a cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the TSF.

FDP_ACF_CIMC.2.2 If certificate subject private keys are stored in the CIMC, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.4 TSF private key confidentiality protection

Hierarchical to: No other components

FMT_MTD_CIMC.4.1 CIMC private keys shall be stored in a cryptographic module or stored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.3 Public Key Storage (Mandatory)

This subsection specifies security requirements that are designed to detect the unauthorized modification of public keys stored in a CIMC. The requirements in this section apply to CIMCs at Security Levels 3 and 4.

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

Hierarchical to: No other components

FDP_SDI_CIMC.3.1 Public keys stored within the TOE, but not within a FIPS 140-1 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_CIMC.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall [ST assignment: *action to be taken*].

Application Note: The ST should specify the actions to be taken in case the verification fails.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.4 Secret Key Storage

Secret (symmetric) keys may be used for several purposes in a CIMC. They may be used to encrypt other secret or private keys when they are stored within or exported from the CIMC. They may also be used to authenticate subscribers (users) and CIMCs. Secret keys must be protected against unauthorized modification and disclosure.

Applicants for certificates may be given PIN or password authenticators. The process for generating and delivering these authenticators to applicants is outside the scope of this document.

The following requirements are mandatory if the CIMC stores secret keys.

FDP_ACF_CIMC.3 User secret key confidentiality protection

Hierarchical to: No other components

FDP_ACF_CIMC.3.1 User secret keys stored within the TOE, but not within a FIPS 140-1 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

Hierarchical to: No other components

FMT_MTD_CIMC.5.1 TSF secret keys stored within the TOE, but not within a FIPS 140-1 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.5 Private and Secret Key Destruction (Mandatory)

This section specifies requirements for the zeroization/destruction of plaintext private and secret keys stored within CIMCs.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [ST assignment: *cryptographic key destruction method*] that meets the following: [ST assignment: *list of standards*].

Application Note: The ST should specify the key destruction method to be used to destroy cryptographic keys. The ST should specify the assigned standard that documents the method used to destroy cryptographic keys. The assigned standard may comprise none, one or more actual standards publications, for example, from international, national, industry or organizational standards.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_CKM_CIMC.5 CIMC private and secret key zeroization

Hierarchical to: No other components.

FCS_CKM_CIMC.5.1 The TSF shall provide the capability to zeroize plaintext secret and private keys within the TOE.

Dependencies: No dependencies.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.6 Private and Secret Key Export

Keys may be exported from cryptographic modules for a variety of reasons, including key backup, replication, and transmission of user private keys generated in CIMCs. There are different requirements for Security Levels 1 and 2 and Security Levels 3 and 4.

SECURITY LEVELS 1 AND 2

FDP_ETC_CIMC.4 User private and secret key export

Hierarchical to: No other components.

FDP_ETC_CIMC.4.1 Electronically distributed private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

FDP_ETC_CIMC.4.2 Certificate subject private keys that are used to generate digital signatures shall not be exported from the CIMC in plaintext form.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.6 TSF private and secret key export

Hierarchical to: No other components.

FMT_MTD_CIMC.6.1 Electronically distributed private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

NOTE: At Security Levels 1 and 2, manually distributed secret and private keys (other than certificate subject private keys that are used to generate digital signatures) may be exported in plaintext form from a CIMC.

SECURITY LEVELS 3 AND 4**FDP_ETC_CIMC.5 Extended user private and secret key export**

Hierarchical to: FDP_ETC_CIMC.4

FDP_ETC_CIMC.5.1 Private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.7 Extended TSF private and secret key export

Hierarchical to: FMT_MTD_CIMC.6

FMT_MTD_CIMC.7.1 Private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.8 Self-tests (Mandatory)

All CIMCs shall implement the following self-tests.

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components

- FPT_AMT.1.1** The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Application Note: The ST author should specify when the TSF will execute the abstract machine testing. The ST author, through this selection, has the ability to indicate the frequency with which the self-tests will be run. If the tests are run often, then the end users should have more confidence that the TOE is operating correctly than if the tests are run less frequently. However, this must be balanced with the potential impact on the availability of the TOE.

Dependencies: No dependencies.

FPT_TST_CIMC.2 Software/firmware integrity test

Hierarchical to: No other components.

- FPT_TST_CIMC.2.1** An error detection code (EDC) or FIPS-approved authentication technique (e.g., the computation and verification of an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware residing within the TOE (e.g., within EEPROM and RAM). The EDC shall be at least 16 bits in length.

- FPT_TST_CIMC.2.2** The error detection code, authentication code, keyed hash, or digital signature shall be verified at power-up and on-demand. If verification fails, the TSF shall [ST assignment: *action to be taken*].

Application Note: The ST should specify the actions to be taken if signature verification fails.

Dependencies: FPT_AMT.1 Abstract machine testing.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria. It satisfies the security objective O.Integrity protection of user data and software.

FPT_TST_CIMC.3 Software/firmware load test

Hierarchical to: No other components

- FPT_TST_CIMC.3.1** A cryptographic mechanism using an authentication technique (e.g., an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware that can be externally loaded into the TOE.

- FPT_TST_CIMC.3.2** The TSF shall verify the authentication code, keyed hash, or digital signature whenever the software or firmware is externally loaded into the TOE. If verification fails, the TSF shall [ST assignment: *action to be taken*].

Application Note: The ST should specify the action to be taken if the signature verification fails.

Dependencies: FPT_AMT.1 Abstract Machine Testing

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria. It satisfies the security objective O.Integrity protection of user data and software.

6.9 Certificate Profile Management (Mandatory)

A certificate profile defines the set of acceptable values for fields and extensions in a certificate. Examples of information that may be specified in a certificate profile include:

- constraints on the key owner's identifier (e.g., subject and/or subjectAltName in X.509);
- the set of allowable algorithms for the subject's public/private key pair;
- the certificate issuer's identifier (e.g., issuer and/or issuerAltName in X.509);
- the limitations on the length of time for which the certificate is valid;
- additional information that may/must be included in a certificate (e.g., which extensions may/must be included in an X.509 certificate);
- whether the subject of the certificate may be a CA;
- the types of operations that may be performed using the private key corresponding to the public key in the certificate (e.g., possible values for keyUsage and/or extKeyUsage in X.509);
- the policy (policies) under which the certificate may/must be issued.

There are two sets of requirements for Certificate Profile Management, Security Level 1 requirements and Security Levels 2, 3, and 4 requirements.

SECURITY LEVEL 1

FMT_MOF_CIMC.2 Certificate profile management

Hierarchical to: No other components.

FMT_MOF_CIMC.2.1 The TOE shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_CIMC.2.2 The TOE shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;
- the identifier of the certificate issuer;
- the length of time for which the certificate is valid;

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.security roles.

SECURITY LEVELS 2, 3, AND 4

FMT_MOF_CIMC.3 Extended certificate profile management

Hierarchical to: FMT_MOF_CIMC.2

FMT_MOF_CIMC.3.1 The TOE shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_CIMC.3.2 The TOE shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;

- the identifier of the certificate issuer;
- the length of time for which the certificate is valid;

FMT_MOF_CIMC.3.2 If the certificates generated are X.509 certificates, the TOE shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- **keyUsage**;
- **basicConstraints**;
- **certificatePolicies**

FMT_MOF_CIMC.3.3 The Administrator shall specify the acceptable set of certificate extensions.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.security roles.

6.10 Certificate Revocation List Profile Management

A certificate revocation list profile is used to define the set of acceptable values for fields and extensions in a CRL. Examples of values that may be covered by a certificate revocation list profile include:

- **extensions** – the set of extensions that may/must be included in a CRL and the value of each extension's criticality bit.
- **issuer, issuerAltName** – the name of the CRL issuer.
- **nextUpdate** – the lifetime of a CRL.

There are two sets of requirements for Certificate Revocation List Profile Management, Security Level 1 requirements and Security Levels 2, 3, and 4 requirements.

SECURITY LEVEL 1

FMT_MOF_CIMC.4 Certificate revocation list profile management

Hierarchical to: No other components.

FMT_MOF_CIMC.4.1 If a CIMC issues CRLs, the TOE must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.

FMT_MOF_CIMC.4.2 TOEs that issue CRLs shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- **issuer**;
- **issuerAltName** (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.)

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Security roles.

SECURITY LEVELS 2, 3, AND 4

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: FMT_MOF_CIMC.4

- FMT_MOF_CIMC.5.1** If a CIMC issues CRLs, the TOE must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.
- FMT_MOF_CIMC.5.2** TOEs that issue CRLs shall require the Administrator to specify the set of acceptable values for the following fields and extensions:
- **issuer;**
 - **issuerAltName** (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.)
 - **nextUpdate** (i.e., lifetime of a CRL).
- FMT_MOF_CIMC.5.3** The Administrator shall specify the acceptable set of CRL and CRL entry extensions.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Security roles.

6.11 Online Certificate Status Protocol (OCSP) Profile Management

An online certificate status protocol profile is used to define the set of acceptable values for the fields in an OCSP response. The OCSP profile may specify the type(s) of responses that the CIMC may generate (i.e., acceptable values for **responseType**) as well as the set of acceptable values for the fields within the acceptable response types. Examples of values that may be covered by an OCSP profile for the basic response type include:

- **ResponderID** - the identifier of the OCSP responder
- **nextUpdate** – limitations on the lifetime of an OCSP response

FMT_MOF_CIMC.6 OCSP profile management

Hierarchical to: No other components.

- FMT_MOF_CIMC.6.1** If a CIMC issues OCSP responses, the TOE must implement an OCSP profile and ensure that issued OCSP responses are consistent with the OCSP profile.
- FMT_MOF_CIMC.6.2** TOEs that issue OCSP responses shall require the Administrator to specify the set of acceptable values for the **responseType** field (unless the CIMC can only issue responses of the basic response type).
- FMT_MOF_CIMC.6.3** If the TOE is configured to allow OCSP responses of the basic response type, the TOE shall require the Administrator to specify the set of acceptable values for the following fields within the basic response type:
- **ResponderID** - the identifier of the OCSP responder
 - **nextUpdate** – limitations on the lifetime of an OCSP response

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Security roles.

6.12 Certificate Registration (Mandatory)

The functions in this section address the validation, approval, and signing of public key certificates.

X.509 public key certificates issued by CIMCs must be compliant with the X.509 standard. Any fields or extensions to be included in an X.509 certificate will either be created by the CIMC according to the rules of the X.509 standard or validated by the CIMC to ensure compliance.

The data entered in each field and extension to be included in a certificate must be approved. Generally, a certificate field or extension value may be approved in one of four ways:

1. The data may be approved manually by an Officer.
2. An automated process may be used to review and approve the data.
3. The value for a field or extension may be automatically generated by the CIMC.
4. The value for a field or extension may be taken from the certificate profile.

FDP_CIMC_CER.1 Certificate Generation

Hierarchical to: No other components.

- FDP_CIMC_CER.1.1** The TSF shall only generate certificates that are consistent with the currently defined certificate profile.
- FDP_CIMC_CER.1.2** The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate.
- FDP_CIMC_CER.1.3** If the TSF generates X.509 certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that:
- a) The **version** field shall contain the integer **0**, **1**, or **2**.
 - b) If the certificate contains an **issuerUniqueID** or **subjectUniqueID** then the **version** field shall contain the integer **1** or **2**.
 - c) If the certificate contains **extensions** then the **version** field shall contain the integer **2**.
 - d) The **serialNumber** shall be unique with respect to the issuing Certification Authority.
 - e) The **validity** field shall specify a **notBefore** value that does not precede the current time and a **notAfter** value that does not precede the value specified in **notBefore**.
 - f) If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **issuerAltName** extension.
 - g) If the **subject** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **subjectAltName** extension.
 - h) The **signature** field and the **algorithm** in the **subjectPublicKeyInfo** field shall contain the OID for a FIPS-approved algorithm.

Dependencies: No dependencies.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

NOTE: The proof-of-possession requirement for certificate subject private keys (FDP_CIMC_CER.1.3) needs to be changed. One method of performing POP for key management keys is to create a certificate and then send the certificate to the certificate subject in encrypted form. The certificate

subject then proves possession of the private key by decrypting the certificate. (This is the indirect method of POP described in section 2.3.2 of RFC 2510). As this POP method requires the CIMC to create the user's certificate before POP has been performed, it is precluded by the requirements as currently stated in FDP_CIMC_CER.1.3.

Since we do not wish to preclude the indirect method of POP for key management keys, we must either find a way to write FDP_CIMC_CER.1.3 that does not preclude this method or remove the requirement to perform POP for key management keys entirely. We would appreciate any suggestions for the wording of FDP_CIMC_CER.1.3.

6.13 Certificate Revocation

The functions in this section address the validation and approval of certificate revocation information.

6.13.1 Certificate Revocation List Validation

Certificate revocation lists (CRLs) issued by CIMCs shall be compliant with the X.509 standard. Any fields or extensions to be included in a CRL shall be created by the CIMC according to the X.509 standard.

FDP_CIMC_CRL.1 Certificate revocation list validation

Hierarchical to: No other components.

- FDP_CIMC_CRL.1.1** The CIMC shall verify that all mandatory fields in the CRL contain values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated:
1. If the **version** field is present, then it shall either contain a **0** or a **1**.
 2. If the CRL contains any critical extensions, then the **version** field shall contain the integer **1**.
 3. If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical **issuerAltName** extension.
 4. The **signature** and **signatureAlgorithm** fields shall contain the OID for a FIPS-approved digital signature algorithm.
 5. The **thisUpdate** field shall indicate the issue date of the CRL.
 6. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.13.2 OCSP Basic Response Validation

OCSP basic responses issued by CIMCs shall be compliant with IETF RFC 2560. Any fields or extensions to be included in an OCSP response shall be created by the CIMC according to IETF RFC 2560.

FDP_CIMC_OCSP.1 OCSP basic response validation

Hierarchical to: No other components.

- FDP_CIMC_OCSP.1.1** The CIMC shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 2560. At a minimum, the following items shall be validated:

1. If the **version** field is present, then it shall contain a **0**.
2. If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical **issuerAltName** extension.
3. The **signatureAlgorithm** field shall contain the OID for a FIPS-approved digital signature algorithm.
4. The **thisUpdate** field shall indicate the time at which the status being indicated is known to be correct.
5. The **producedAt** field shall indicate the time at which the OCSP responder signed the response.
6. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.14 Cryptographic Modules

In many cases, a CIMC may use a single cryptographic module to perform all cryptographic functions. However performance and cost considerations may require a design that uses several separate cryptographic modules performing distinct functions. For example, a level 3 CIMC might use a hardware cryptographic module validated to FIPS 140-1 level 3 to sign certificates and CRLs, but use a software cryptographic module that has only been validated to level 2 to compute authentication codes for general transaction messages.

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: *encryption, decryption, signature generation, signature verification, authentication code generation, authentication code verification, hash generation, hash verification*] in accordance with a specified FIPS-approved algorithm that meets a FIPS standard.

Application Note: The ST should specify the cryptographic operations that are being performed.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

In Section 6.15.2 below, cryptographic functions and keys are categorized based on their uses within a CIMC. Security requirements are then imposed on the cryptographic modules within a CIMC based on the Security Level of the CIMC, the types of cryptographic functions that are performed by the cryptographic module, and the types of keys that are stored within the cryptographic module.

6.15 Operating System

Typically, most CIMCs will implement at least one cryptographic function in software (even if it is just computing a SHA-1 hash to be signed by a hardware cryptographic module). Any CIMC that implements cryptographic functions in software will need to meet the Operating System requirements of FIPS 140-1&2. The operating system requirements are required, "...only if the module provides a means whereby an

operator can load and execute software or firmware that was not included as part of the validation of the module.” At Security Levels 2 through 4, FIPS 140-1&2 require an evaluated operating system. The evaluation will be against the CC (or an equivalent standard). Therefore, it is important to maintain consistency between the Operating System requirements for CIMCs and the Operating System requirements for cryptographic modules.

FIPS 140-1 is currently undergoing a 5-year review process. The Operating System requirements in FIPS 140-2 have not yet been finalized, but will differ from those in FIPS 140-1. As the Operating System requirements for FIPS 140-2 are finalized, we will revise the Operating System requirements for this document.

6.16 Strength of Function

6.16.1 Authentication Mechanisms

The authentication mechanisms specified in FIA_UAU.1 shall meet the following strength of function requirements:

- 1 For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods.)
- 2 For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

6.16.2 Cryptographic Modules

FIPS 140-1 validated cryptographic modules must perform all cryptographic functions performed by CIMCs. FIPS 140-1 validated cryptographic modules are also required to generate cryptographic keys and to store plaintext private and secret keys.

6.16.2.1 Encryption and FIPS 140-1 Validated Modules

6.16.2.1.1 Encryption Algorithms

The encryption specified for:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification of origin
FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_CIMC_BKP.2	Extended CIMC backup and recovery
FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export
FPT_CIMC_TSP.1	Audit log time stamp event
FPT_TST_CIMC.2	Software/firmware integrity test
FPT_TST_CIMC.3	Software/firmware load test

shall be performed using a FIPS-approved algorithm.

6.16.2.1.2 FIPS 140-1 Validated Cryptographic Modules

Cryptographic modules specified for:

FCS_CKM.1	Cryptographic key generation
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export

shall be validated against FIPS 140-1.

6.16.2.1.3 Split Knowledge Procedures

Split-knowledge procedures specified in:

FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export

shall be implemented and validated as specified in FIPS 140-1.

6.16.2.1.4 Authentication Codes

The authentication code specified in:

FAU_STG.1	Protected audit trail storage
FDP_CIMC_BKP.2	Extended CIMC backup and recovery
FCO_NRO_CIMC.4	Advanced verification of origin
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FPT_TST_CIMC.2	Software/firmware integrity test
FPT_TST_CIMC.3	Software/firmware load test

shall be a FIPS-approved authentication code.

All cryptographic operations performed by the TOE shall be performed in a FIPS 140-1 validated cryptographic module operating in a FIPS-approved mode of operation.

Table 6 specifies for each category of use for a private or secret key and CIMC Security Level, the required overall FIPS 140-1 level for the validated cryptographic module.

Table 6: FIPS 140-1 Security Level for Validated Cryptographic Module

Required Overall FIPS 140-1 Level for CIMC Cryptographic Modules				
Category of Use	CIMC Security Level 1	CIMC Security Level 2	CIMC Security Level 3	CIMC Security Level 4
<i>Certificate and Status Signing</i>				

- single party signature	1	2	3	4
- multiparty signature	1	1	2	3
<i>Integrity or Approval Authentication</i>				
- single approval	1	2	2	3
- dual approval	1	1	2	2
<i>General Authentication</i>	1	1	2	2
<i>Long Term Private Key Protection</i>	1	2	3	4
<i>Long Term Confidentiality</i>	1	1	2	2
<i>Short Term Private key Protection</i>	1	1	2	2
<i>Short Term Confidentiality</i>	1	1	1	2

The Security Level of the validated cryptographic module will be selected from the above table using the CIMC level (column) and the category of use (row). For example, if the CIMC level is 2 and the key is used for general authentication, the cryptographic module must be validated to FIPS 140-1 Security Level 1.

6.16.2.2 Cryptographic Functions That Do Not Involve Private or Secret Keys

There are two other cryptographic functions that may be performed in CIMCs that do not require private or secret keys. These include:

1. *Hash Generation*: One-way hash functions may be used in the process of signature generation and verification (a signature is typically generated by applying a private key to the hash of the message). The generation of a hash does not require a key. Therefore, hash generation does not have the same confidentiality requirements of other cryptographic functions.
2. *Signature Verification*: Signatures are verified from a message text and a public key.

For a cryptographic module that only performs signature verification and/or keyless hash generation functions, the overall required FIPS 140-1 Security Level shall be Security Level 1 for CIMC Levels 1 through 3 and Security Level 2 for CIMC Level 4.

7 TOE Security Assurance Requirements

This section specifies the assurance requirements for CIMCs. Details of the assurance components specified in this section may be found in part 3 of the Common Criteria.

7.1.1 Security Level 1 Security Assurance

The assurance requirements for CIMCs at Security Level 1 are the requirements for EAL1 with the addition of ATE_FUN.1 Functional Testing and AVA_SOF.1 Strength of TOE Security Function Evaluation. These requirements are designed to provide evidence that the CIMC functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

The assurance requirements for Security Level 1 are summarized below.

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.1	Version numbers
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance

Assurance Class	Component ID	Component Title
	AGD_USR.1	User Guidance
Tests	ATE_FUN.1	Functional Testing
	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation

7.1.2 Security Level 2 Security Assurance

The assurance requirements for CIMCs at Security Level 2 are those specified in *CSPP - Guidance for COTS Security Protection Profiles*.³ The assurance requirements of CSPP, which shall be referred to as EAL-CSPP, stress assurance through vendor actions that are within the bounds of current best commercial practice. EAL-CSPP provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CSPP also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented, (3) verification of a sample of the vendor functional testing, (4) searching for obvious vulnerabilities, and (5) independent functional testing.

The assurance requirements for EAL-CSPP are summarized below.

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM Coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing - High-Level Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.1	Developer vulnerability Analysis

³ Version 1.0 of *CSPP - Guidance for COTS Security Protection Profiles* (NISTIR 6462) may be obtained from <http://csrc.nist.gov/cc/pp/pplist.htm#CSPP>.

7.1.3 Security Level 3 Security Assurance

The assurance requirements for CIMCs at Security Level 3 are extracted from EAL Levels 3 and 4, with the addition of ALC_FLR.2: Flaw reporting procedures. CIMC Security Level 3 includes all of requirements from CC EAL3, augmenting many of the EAL3 requirements. Of the 22 CIMC Security Level 3 requirements, 12 are from EAL3, 9 are from EAL4, and one (ALC_FLR.2) does not appear in any of the EAL levels.

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

7.1.4 Security Level 4 Security Assurance

The assurance requirements for CIMCs at Security Level 4 are extracted from EAL Levels 4 and 5, with the addition of ALC_FLR.3: Systematic flaw remediation. Of the 25 requirements, 21

are from EAL4, 3 are from EAL5, and one (ALC_FLR.3) does not appear in any of the EAL levels.

Assurance Class	Component ID	Component Title
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures

Assurance Class	Component ID	Component Title
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_INT.1	Modularity
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

8 Rationale

8.1 IT Security Objectives Rationale

IT Security Objective	Threat
O.Administrators, Operators, Officers and Auditors guidance documentation	T.Administrators, Operators, Officers, and Auditors commit errors, T.Disclosure of private and secret keys
O.Apply patches to fix the code	T.Hacker undetected system access
O.Audit records with identity	T.Hacker masquerading as a legitimate user or a system process, T.Hacker undetected system access, T.User abuses authorization to collect data, T.User abuses authorization to send data
O.Audit system access to deter misuse	T.Hacker undetected system access
O.Auditing for user accountability	T.Administrative errors of omission
O.Auditor role	T.Administrators, Operators, Officers, and Auditors commit errors T.Hostile Administrator, Operator, Officer, or Auditor actions

O.Authorization	T.Administrators, Operators, Officers, and Auditors commit errors, T.User abuses authorization to collect data, T.User abuses authorization to send data
O.Certificates	T.Administrators, Operators, Officers, and Auditors commit errors
O.Code signing and verification	T.TOE developed with inadequate TSF self protection, T.Modification of secret/private keys
O.Configuration management	T.Critical system component fails, T.Malicious code exploitation, T.TOE developed with inadequate TSF self protection
O.Control unknown source communication traffic	T.Hacker undetected system access
O.Cryptographic algorithms	T.Weak cryptographic algorithms
O.Data Import/Export	T.User abuses authorization to send data
O.Detect modifications of backup hardware, firmware, and software	T.Hostile Administrator, Operator, Officer, or Auditor actions
O.Protected user authentication data	T.Hacker undetected system access, T.Hostile Administrator, Operator, Officer, or Auditor actions
O.Enforcement	T.Disclosure of private and secret keys, T.TOE developed with inadequate TSF self protection
O.Examine source code for developer flaws	T.Flawed code, T.TOE developed with inadequate TSF self protection
O.General user documentation	T.Social engineering
O.Guarantee the availability of audit storage space	T.Hacker undetected system access
O.Identify and authenticate each user	T.Hacker undetected system access, T.Hostile Administrator, Operator, Officer, or Auditor actions
O.Individual accountability	T.Hacker undetected system access, T.Hostile Administrator, Operator, Officer, or Auditor actions, T.User abuses authorization to collect data, T.User abuses authorization to send data
O.Integrity protection of user data and software	T. Malicious code exploitation, T.Modification of private/secret keys
O.Isolate untrusted executables	T.Malicious code exploitation
O.Key generation	T.Disclosure of private and secret keys, T.Weak cryptographic algorithms
O.Lifecycle security	T.Critical system component fails, T. Malicious code exploitation, T.Social engineering
O.Limitation of administrative access control	T.Hostile Administrator, Operator, Officer, or Auditor actions
O.Local detection of received security-relevant data modified in transit	T.Message content modification
O.Maintain user attributes	T.Administrators, Operators, Officers, and Auditors commit errors
O.Manage behavior of security functions	T.Administrators, Operators, Officers, and Auditors commit errors, T.Critical system component fails, T.Hostile Administrator, Operator, Officer, or Auditor actions, T.User's misuse causes denial of service
O.Manage security-relevant data	T.Hacker undetected system access
O.Non-repudiation	T.Sender denies sending information
O.Notify authorities of security issues	T.Administrative errors of omission, T.Hostile Administrator, Operator, Officer, or Auditor actions, T.User error makes data inaccessible
O.Object and data recovery free from malicious code	T.Malicious code exploitation, T.Modification of secret/private keys

O.Operator/Administrator access	T.Hostile Administrator, Operator, Officer, or Auditor actions
O.Periodically check integrity	T.Malicious code exploitation
O.Preservation of secure state for failures in critical components	T.Critical system component fails
O.Procedures for preventing malicious code	T.Social engineering
O.Protect stored audit records	T.Hostile Administrator, Operator, Officer, or Auditor actions, T.Modification of secret/private keys
O.Protect user data during internal transfer	T.Flawed code, T.User abuses authorization to collect data
O.React to detected attacks	T.Hacker undetected system access
O.Require inspection for downloads	T.Malicious code exploitation
O.Respond to possible loss of stored audit records	T.Administrators, Operators, Officers, and Auditors commit errors
O.Restrict actions before authentication	T.Administrators, Operators, Officers, and Auditors commit errors
O.Robust encryption	T.Weak cryptographic algorithms
O.Security roles	T.Administrators, Operators, Officers, and Auditors commit errors
O.Security-relevant configuration management	T.Administrative errors of omission
O.Sufficient backup storage and effective restoration	T.Critical system component fails
O.Tamper detection	T.Administrators, Operators, Officers, and Auditors commit errors
O.Time stamps	T.Hostile Administrator, Operator, Officer, or Auditor actions, T.Critical system component fails
O.Trusted path	T.Hacker undetected system access, T.Hacker masquerading as a legitimate user or a system process, T.User abuses authorization to collect data
O.Trusted recovery of security functionality	T.Critical system component fails
O.User authorization management	T.Administrative errors of omission
O.Validation of security function	T.Hostile Administrator, Operator, Officer, or Auditor actions, T.Malicious code exploitation

8.2 Non-IT Security Objectives Rationale

Non-IT Security Objective	Threat
O.Administrative Training	T.Administrators, Operators, Officers, and Auditors commit errors
O.CPS	
O.Credentials	
O.Installation	T.Critical system component fails
O.Physical Protection	T.Hacker physical access

8.3 Functional Security Requirements Rationale

Functional Requirement	Objective
ALC_FLR.2 Flaw reporting procedures	O.Examine source code for developer flaws
AGD_ADM.1 Administrator Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.Procedures for

	preventing malicious code, O.Validation of security function
AGD_USR.1 User Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.General user documentation, O.Procedures for preventing malicious code
FDP_CIMC_ARC.1 CIMC archive	O.Sufficient archive storage and effective restoration
FDP_CIMC_ARC.2 Extended CIMC archive	O.Preservation of secure state for failures in critical components, Trusted recovery of security function
FDP_CIMC_ARC.3 Advanced CIMC archive	O.Preservation of secure state for failures in critical components, Trusted recovery of security function
FDP_CIMC_BKP.1 CIMC backup and recovery	O.Sufficient backup storage and effective restoration
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	O.Detect modifications of backup hardware, firmware, and software, O.Preservation of secure state for failures in critical components, O.Trusted recovery of security function
FDP_CIMC_BKP.3 Advanced CIMC backup and recovery	O.Detect modifications of backup hardware, firmware, and software, O.Preservation of secure state for failures in critical components, O.Trusted recovery of security function
FAU_GEN.1 Audit data generation	O. Audit records with identity, O.Auditing for user accountability, O.Individual accountability
FAU_GEN.2 User identity association	O.Audit system access to deter misuse, O.Auditing for user accountability
FAU_SAR.1 Audit review	O.Audit system access to deter misuse, O.Auditing for user accountability
FAU_SAR.3 Selectable audit review	O.Auditing for user accountability, O.Notify authorities of security issues
FAU_SEL.1 Selective audit	O. O.Audit system access to deter misuse, O.Auditing for user accountability
FAU_STG.1 Protected audit trail storage	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss	O.Respond to possible loss of stored audit records
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	O.Non-repudiation
FCO_NRO_CIMC.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM.1 Cryptographic key generation	O.Cryptographic algorithms, O.Robust encryption
FCS_CKM.4 Cryptographic key destruction	O.React to detected attacks, O.Tamper detection
FCS_CKM.CIMC.5 CIMC private and secret key zeroization	O.React to detected attacks, O.Tamper detection
FCS_COP.1 Cryptographic operation	O.Robust encryption, O.Key generation
FDP_ACC.1 Subset access control	O. Require inspections for downloads, O.Limitation of administrative access control
FDP_ACF_CIMC.2 User private key confidentiality protection	O.Protected user authentication data, O.Robust encryption
FDP_ACF_CIMC.3 User secret key confidentiality protection	O.Protected user authentication data
FDP_ETC_CIMC.4 User private and secret key export	O.Data import/export, O.Robust encryption
FDP_ETC_CIMC.5 Extended user private and secret key export	O.Data import/export, O.Robust encryption
FDP_CIMC_CER.1 Certificate Generation	O.Certificates

FDP_CIMC_CRL.1 Certificate revocation list validation	O.Certificates
FDP_CIMC_CSE.1 Certificate status export	O.Certificates
FDP_ITT.1 Basic internal transfer protection	O.Integrity protection of user data and software, O.Protect user data during internal transfer
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	O.Integrity protection of user data and software
FDP_UCT.1 Basic data exchange confidentiality	O.Data Import/Export
FIA_AFL.1 Authentication failure handling	O.React to detected attacks
FIA_ATD.1 User attribute definition	O.Auditing for user accountability
FIA_UAU.1 Timing of authentication	O.Code signing and verification, O.Control unknown source communication traffic, O.Operator/Administrator access, O.Restrict actions before authentication
FIA_UID.1 Timing of identification	O.Identify and authenticate each user, O.Individual accountability, O.Operator/Administrator access
FIA_USB.1 User-subject binding	O.Auditing for user accountability, O.Identify and authenticate each user, O.Individual accountability,
FMT_MOF.1 Management of security functions behavior	O.Apply patches to fix the code, O.Auditing for user accountability, O.Configuration management, O.System archive procedures, O.Backup procedures, O.Manage behavior of security functions, O.Security-relevant configuration management
FMT_MOF.CIMC.2 Certificate profile management	O.Configuration management
FMT_MOF.CIMC.3 Extended certificate profile management	O.Configuration management
FMT_MOF.CIMC.4 Certificate revocation list profile management	O.Configuration management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	O.Configuration management
FMT_MSA.1 Management of security attributes	O.Apply patches to fix the code, O.Maintain user attributes, O.Manage resource security attributes, O.User authorization management
FMT_MSA.2 Secure security attributes	O.Manage resource security attributes, O.Security-relevant configuration management
FMT_MSA.3 Static attribute initialisation	O.Manage resource security attributes, O.Security-relevant configuration management
FMT_MTD.1 Management of TSF data	O.Configuration management, O.System archive procedures, O.Backup procedures, O.Manage security-relevant data, O.Security-relevant configuration management
FMT_MTD_CIMC.4 TSF private key confidentiality protection	O.Security-relevant configuration management
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	O.Security-relevant configuration management
FMT_MTD_CIMC.6 TSF private and secret key export	O.Data import/export, O.Security-relevant configuration management
FMT_MTD_CIMC.7 Extended TSF private and secret key export	O.Data import/export, O.Security-relevant configuration management
FMT_SMR.2 Restrictions on security roles	O.Auditor role, O.Auditing for user accountability, O.Security roles
FPT_AMT.1 Abstract machine testing	O.Periodically check integrity
FPT_ITC.1 Inter-TSF confidentiality during	O.Data Import/Export

transmission	
FPT_ITT.1 Basic internal TSF data transfer protection	O.Protect user data during internal transfer
FPT_STM.1 Reliable time stamps	O.Time stamps
FPT_CIMC_TSP.1 Audit log time stamp event	O.Time stamps
FPT_TST_CIMC.2 Software/firmware integrity test	O.Object and data recovery free from malicious code, O.Periodically check integrity
FPT_TST_CIMC.3 Software/firmware load test	O.Object and data recovery free from malicious code, O.Periodically check integrity
FTP_TRP.1 Trusted path	O.Trusted path

8.4 Security Policy Rationale

Security Policy	Objective
P.Authorized use of information	O.Auditor role O.Maintain user attributes O.Operator/Administrator access O.Restrict actions before authentication O.Security roles O.User authorization management
P.Cryptography	O.Cryptographic algorithms O.Data Import/Export O.Key generation O.Robust encryption
P.Individual accountability	O.Individual Accountability O.Audit records with identity O.Audit system access to deter misuse O.Audit for user accountability O.Identify and authenticate each user
P.Information access control	O.Discretionary access control O.Protected user authentication data O.Limitation of administrative access control O.Manage behavior of security functions O.Manage security-relevant data
P.Information availability	O.Configuration management O.Control unknown source communication traffic O.Detect modifications of backup hardware, software, and firmware O.Procedures for preventing malicious code O.Sufficient archive storage and effective restoration O.Sufficient backup storage and effective restoration O.System archive procedures O.System backup procedures O.Trusted recovery of security functionality O.Validation of security function
P.Information content integrity	O.Certificates O.Code signing and verification O.Configuration management O.Integrity protection of user data and software O.Local detection of received security-relevant data modified in transit O.Non-repudiation

	O.Time stamps
P.Installation and usage guidance	O.Administrators, Operators, Officers and Auditors guidance documentation O.General user documentation O.Non-repudiation
P.Notification of threats and vulnerabilities	O.Notify authorities of security issues O.React to detected attacks O.Tamper detection
P.System lifecycle phases integrate security	O.Apply patches to fix the code O.Enforcement O.Examine source code for developer flaws O.Guarantee the availability of audit storage space O.Isolate untrusted executables O.Lifecycle security O.Manage resource security attributes O.Object and data recovery free from malicious code O.Preservation of secure state for failures in critical components O.Protect stored audit records O.Require inspection for downloads O.Respond to possible loss of stored audit records O.Security-relevant configuration management O.Trusted path

9 CIMC ACCESS CONTROL POLICY

The TOE shall support the administration and enforcement of a CIMC access control policy that provides the capabilities described below.

Subjects (human users) will be granted access to objects (data/files) based upon the:

1. Identity of the subject requesting access,
2. Role (or roles) the subject is authorized to assume,
3. Type of access requested,
4. Content of the access request, and,
5. Possession of a secret or private key, if required.

Subject identification includes:

- Individuals with different access authorizations
- Roles with different access authorizations
- Individuals assigned to one or more roles with different access authorizations

Access type, with explicit allow or deny:

- Read
- Write
- Execute

For each object, an explicit owning subject and role will be identified. Also, the assignment and management of authorizations will be the responsibility of the owner of an object or a role(s), as specified in this PP.

10 (Preliminary) Glossary of Terms⁴

The following definitions are used throughout this standard:

Authentication code: a cryptographic checksum, based on a FIPS-approved security method; also known as a Message Authentication Code (MAC) in ANSI standards.

CIMC: the set of hardware, software, firmware, or some combination thereof, that issues, revokes, and manages public key certificates and certificate status information, and is contained within the CIMC boundary.

CIMC boundary: an explicitly defined contiguous perimeter that establishes the physical bounds of a CIMC.

Compromise: the unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: the property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a CIMC or the security of the information protected by the CIMC.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- a keyed hash computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic key component (key component): a parameter used in conjunction with other key components in a FIPS-approved security method to form a plaintext cryptographic key or perform a cryptographic function.

Data path: the physical or logical route over which data passes; a physical data path may be shared by multiple logical data paths.

Digital signature: a non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.

Encrypted key: a cryptographic key that has been encrypted with a key encrypting key, a PIN or a password in order to disguise the value of the underlying plaintext key.

Error detection code (EDC): a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

FIPS-Approved mode of operation: a mode that employs only the operation of FIPS-approved security methods.

⁴ The terms in this standard are based on terms defined in FIPS PUBs. The terms have been tailored for a CIMS.

FIPS-approved security method: a security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, authentication technique, or evaluation criteria) that is either a) specified in a FIPS or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

Firmware: the programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution.

Hardware: the physical equipment used to process programs and data in a CIMC.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Interface: a logical section of a CIMC that defines a set of entry or exit points that provide access to the CIMC, including information flow or physical access.

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, passwords) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

Microcode: the elementary computer instructions that correspond to an executable program instruction.

Output data: information that is to be exported from a CIMC.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal Identification Number (PIN): a 4 or more character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

Physical protection: the safeguarding of a CIMC, cryptographic keys, or other CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Port: a functional unit of a CIMC through which data or signals can enter or exit the module. Physically separate ports do not share the same physical pin or wire.

Private key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Protection Profile: an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. (Public keys are not considered CSPs.)

Public key certificate: a set of data that unambiguously identifies an entity, contains the entity's public key, is digitally signed by a trusted party, and binds the public key to the entity.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Removable Cover: a cover designed to permit physical access to the contents of a CIMC.

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does

not imply a classification level rather the term implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Security policy: a precise specification of the security rules under which a CIMC shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.

Seed key: a secret value used to seed a cryptographic function or operation.

Software: the programs and associated data that can be dynamically written and modified.

Split knowledge: a condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

Status information: information that is output from a CIMC for the purposes of indicating certain operational characteristics or states of the CIMC.

System software: the special software (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.

Tamper detection: the automatic determination by a CIMC that an attempt has been made to compromise its physical security.

Tamper evidence: the indication that physical tampering of the CIMC has occurred.

Tamper response: the automatic action taken by a CIMC when it detects that physical tampering has occurred (minimum response action is the zeroization of keys and other CSPs).

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Trusted path: a means by which an operator and a TSF can communicate with the necessary confidence to support the TSP.

User: an individual, or a process (subject) operating on behalf of the individual, accessing CIMC.

Zeroization: a method of erasing electronically stored data by altering or deleting the contents of the data storage so as to prevent the recovery of the data.

11 Acronyms

ANSI	American National Standards Institute
CA	Certification Authority
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
CIMC	Certificate Issuing and Management Component
CIMS	Certificate Issuing and Management System
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MISPC	Minimum Interoperability Specification for PKI Components
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
PKIX	PKI for the Internet using X.509 Certificates
PP	Protection Profile
RA	Registration Authority
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy